ANALYSING AND DESIGN A SAFETY MECHANISM ALGORITHM BASED ON THE INTERNET OF THINGS (IoT) FOR HOME(S)

Submitted to

IIMT University

IIMT UNIVERSITY
MEERUT

By

Shailendra Kumar Mani Tripathi

Under the Supervision of

Dr. Pushpendra Kumar Verma

School of Computer Science & Applications

IIMT University, Meerut (U.P.)

Contents

Abstract 3

1.0. Introduction 4

1.1. The Problem 4

1.2. Gap in the Body of Knowledge and Motivation for Research 5

1.3. Aim and research questions. 6

1.4. Objectives of the study 7

1.5. Theoretical Background 7

1.5. Scope of the study 8

1.5.1. Access Control 9

1.5.2. Intrusion Detection 9

1.5.3. Fire and Hazard Detection 10

1.5.4. Emergency Response 10

1.6. Literature Review 11

1.6.1. Cybersecurity Risks for IoT-Based Home Safety Systems 12

1.6.2. Emerging Technologies for IoT Security 13

1.7. Research Methodology 18

1.8. References 19

Abstract

IOT based devices have transformed the lifestyle of household by facilitating convenience and energy efficiency. Besides these advantages these devices posses' security threat as the systems are vulnerable to cyber threats. Primarily due to inadequate security protocols and absence of standardized security measures. Therefore, safety of IOT based devices and home security are concerns for which effective effective security mechanisms. Therefore, the study aims to develop safety mechanism algorithms focused on home-based Internet of Things (IoT) applications. The research focuses on identifying key security constraints with IoT devices in residential settings and aims to evaluate the efficacy of current safety measures. By doing so the purpose of this research is to develop a machine learning algorithm by using variables e.g., access control, intrusion detection. Furthermore, the research would evaluate efficiency of the safety algorithm with help of simulations and real-world tests.

The research identifies the security challenges associated with IoT devices and critically evaluates security mechanisms that has been developed in past. After evaluating the extant literature, it was identified that there is a need for standardized security protocols. Additionally, there is a need to develop guidelines for IoT device manufacturers to develop more effective security mechanisms. The study contributes to creation of effective safety algorithms for IoT devices in residences that would enhance security and safety of such devices. The results of this study will help IoT device manufacturers, security experts, and policymakers to develop enhanced security measures to safeguard against cyber threats.

1.0.Introduction

Application of Internet of Things (IoT) with home appliances has significantly transformed the lives of individuals [1, 2]. These devices have enhanced the efficiency of home security systems. Besides these systems have become vulnerable to the threat of cyber security. This is because vulnerability in any device compromises home's security [3, 4]. These challenges make safety of these devices and home security a primary area of concern for researchers and practitioners alike. Therefore, the study aims develop a machine learning based security protocol for improve home security. The study will extend the algorithms proposed by Georgia, Evangelia [5], Gill, Garraghan [6]. In this process the research would analyse the constraints with current security systems and would identify different types of cyber-attacks that make home security systems vulnerable. This would enhance the safety and security of households that use IoT devices.

1.1. The Problem

In recent years, there has been a notable surge in the adoption of IoT devices within households. These devices, such as smart thermostats, security cameras, and voice assistants, offer a variety of benefits that augment the quality of life for residents[7, 8]. For example, smart thermostats can learn the temperature preferences of a household and autonomously adjust them to ensure optimal comfort. And security cameras can monitor home and alert residents of any potential security breaches [9, 10]. But integration of these devices into managing home creates new security risks of data theft [11]. This is primarily due to cyber-attacks which increases the concern of home owner [12]. Therefore, there is need of an effective safety mechanism that can safeguard these devices from cyber threats.

Current safety mechanisms in IoT based homes security devices use encryption and authentication techniques to secure data transmission between devices and cloud services [13]. However, effectiveness of these mechanism remains a concern as cyber attackers

identify new vulnerabilities to exploit [14]. One such example is in 2016 when Mirai botnet compromised IoT devices making them vulnerable to distributed denial of service (DDoS) attacks causing widespread disruptions on the internet. The attack was successful because many IoT devices lacked basic security features e.g., password protection Ramadan, Huang [15].

To address these challenges the research aims to develop machine learning based algorithms for home security to address the vulnerability of Internet of Things (IoT) based devices. As part of this challenges associated with current safety mechanisms would be identified based and solution from experts would be sought. They solution would be used to develop a machine learning algorithm which would be further validated. The research employs a quantitative approach and real time simulations would be performed to test proposed algorithms.

1.2. Gap in the Body of Knowledge and Motivation for Research

The incorporation of IoT technology into homes has enabled the development of smart home automation, providing homeowners with greater convenience, efficiency, and control [16-18]. While several studies have focused on the technical aspects of IoT devices, such as communication protocols [19-21] and security [22-26], there is still a significant gap in the body of knowledge regarding the development of intelligent algorithm-based systems for home automation using IoT as observed from the works of Hui, Sherratt [3], Kaur, Singh [4], Nasir, Muhammad [11] and Luperto, Monroy [9].

Developing intelligent algorithms for home automation poses several challenges, including the heterogeneity of devices, the variability of the environment, and the need for real-time data processing [8, 27, 28]. Existing smart home automation systems often rely on pre-programmed schedules or user input to control devices, restricting their capacity to adjust to evolving environments and user requirements [4].

Furthermore, the development of intelligent algorithm-based systems requires a deep understanding of the interaction between different devices and the environment to ensure optimal efficiency and reliability [29-31]. Such systems must also be scalable, interoperable, and user-friendly to support a diverse range of devices and use cases [32-34]. Addressing this gap would enhance the efficiency and reliability of automated home security systems. Additionally, use of ML would help in developing intelligent algorithmic systems the would be capable to automate tasks e.g., temperature regulation, lighting adjustments, and security measures in real time. Furthermore, these can also be advanced to optimize energy usage which would reduce overall expenditure and will enhance user experience as observed by Sinha and Dhanalakshmi [35], Sivarajan and Sundarsingh Jebaseelan [36]. Therefore, developing and intelligent algorithm would contribute towards ensure efficient facility management in households.

This is the motivation for exploring intelligent algorithm-driven systems will not only ensure the security but also with the help of IOT integration foster holistic home automation. Therefore, the research will also address the challenges associated with this emerging field based on the stakeholders perspective. As use of such systems would significantly enhance the efficiency home automation which will improve the quality of life for homeowners.

1.3. Aim and research questions.

This research aims to develop a ML based algorithm that utilizing Internet of Things (IoT) technology to enhance home security. Following research question would be addressed as part of this study:

- What safety mechanisms are used in IoT devices for home security?
- What are the common challenges that influence the performance existing safety mechanism in IoT devices?
- What cyber-attacks have target IoT devices in homes?

- What should be key features of an effective algorithmic that would secure IoT devices in homes?
- How can the effectiveness of these algorithms be evaluated?

1.4. Objectives of the study

Following are the objectives of the study:

- To explore the current safety mechanisms being used in IoT devices for home security.
- To identify the challenges associated with the current safety mechanisms in IoT devices.
- To analyze prevalent cyber-attacks that target IoT devices in residential settings.
- To propose effective algorithmic approaches for securing IoT devices in homes.
- To evaluate the effectiveness of these algorithms in securing IoT devices in homes.

1.5. Theoretical Background

The rapid development of the Internet of Things (IoT) has made it possible to deploy smart devices in homes, which facilitates convenience and energy saving [8, 27]. On the other hand, because of their increased connectivity, modern medical devices are more insecure and hence subjected to attacks with repercussions towards human health (cyber-attacks) making this topic a critical issue in healthcare for certain researchers' circles as well as policy makers becoming focused on these issues (Broader impacts: providing aid in identifying proper countermeasures against CPR clue theft.) [28]. This has made the IoT devices a very vulnerable target for attackers due to their low-security protocols and unavailability of standardized security mechanisms.

In 2016 attackers used the Mirai botnet to launch attacks on IoT devices like routers and cameras — infecting hundreds of thousands globally with malware that resulted in a colossal, distributed denial-of-service (DDoS) attack, which crippled whole major websites and services worldwide (Kaspersky, 2017). This raised questions about how secure IoT devices are and whether we need better security mechanisms, desperately. Security

Mechanisms: Several mechanisms have been proposed to address the security challenges faced by IoT devices [37] These mechanisms include encryption, access control or intrusion detection and machine learning based security mechanisms [38]. Encryption is used to secure the transmission of data between devices and cloud, as well access control that around limiting unauthorized user. Intrusion detection system are used to identify potential security breaches [39]. Artificial intelligence-based Security mechanism that using the machine learning to analyses a huge amount of data and identify possible threats (Sikdar et al).

Studies have shown that access control mechanisms, such as password-based authentication, can effectively protect IoT devices from unauthorized access (Alzahrani et al., 2020). However, these mechanisms may not be sufficient to protect against more advanced attacks, such as malware injection and denial-of-service attacks (Amin et al., 2019). Intrusion detection mechanisms can effectively detect potential security breaches, but they may generate false alarms, leading to unnecessary responses that can disrupt normal device operations (Mekki et al., 2018).

Machine learning techniques have already started to be applied successfully in improving the security of IoT devices as ideally, they could analyze device behaviour over time, which would detect any strange activities (Sundaravadivel et al., 2021). Such mechanisms are also flexible to evolve with new threats and be able to provide more fine-grained protection for IoT devices against cyber-attacks [9, 40]. But, creating a robust machine learning-based security framework for IoT devices present certain challenges because such frameworks need large sets of training data and computational resources (Chakraborty et al., 2020).

Hence, there is a great urgency to build uniform security policies and standards for IoT device makers to safeguard home security [10, 41, 42]. This could result in greater security of IoT devices and hence bring down the potential cyber-attack risk. Furthermore, more research is required to design new security approaches that can defend against the

future and easily adapt to different environments. It is therefore not surprising that introducing IoT devices into homes has provided numerous benefits but at the same time, introduces new risks of attack. To defend against cyber-attacks and guarantee the security, trustworthiness of IoT devices we require robust security solutions [11, 12, 43]. Developing uniform security protocols and policies can ensure a secure IoT device protection regime, but further study is necessary to make this facility more powerful. The following sections will describe some of the basic terminology in IOT.

Scope of the study

1.5.1. Access Control

The research could have far-ranging implications in the development of algorithms and protocols for home access control with IoT devises, akin to using biometrics or electronic keyless doorways. Of course, the algorithms would also have to be secure and trustworthy so that no second-party could attempt any kind of hacking. Researchers will look at different types of biometrics such as facial recognition and fingerprint scanning to see how successful they are in preventing unwarranted access. It would also look at how to better interconnect access control systems with other IoT devices, like smart locks in the home that could lead improve homeowner security collectively.

1.5.2. Intrusion Detection

They study would focus on how IoT sensors and devices for watching out possible intruders or triggers security alarms. The research would also examine various sensors, think motion detectors and cameras or microphones etc., establish detection algorithms to masturbate-developer the sensor data into which someone has entered. A separate motion- or sound-activated study would try to differentiate between an unwelcome human in a home and other sources of motion/sound — like pets, trees blowing outside windows or cars passing on the street—to eliminate false alarms. Moreover, the research would also explore methods to fuse

an intrusion detection system with a smart light or alarm that informs us if there is any suspecting presence.

1.5.3. Fire and Hazard Detection

Among other things, the study would investigate how to deploy new types of sensors in the home (think smoke and gas leak detectors) that could rapidly respond if a disaster is about to take place. This project would develop algorithms to analyze data received from sensors (like smoke detectors or gas detectors) and take proper actions when needed like setting off alarms, turning of the distributing lines for flammable gases. The research would also consider how to couple hazard detection systems with other IoT devices, such as smart thermostats or sprinkler systems that could stop a fire from spreading before anyone notices it.

1.5.4. Emergency Response

The research, for example, would investigate how IoT devices could rapidly notify emergency services in the event of a fire, break-in or other emergencies. The project, if carried to fruition in actual products, would build algorithms that can identify when an emergency is taking place and sufficiently important enough for them to hit the button (whether contacting emergency service or sending out a message over your smartphone. This research would also focus on possible emergency response systems that could be integrated with other IoT devices, such as medical alert appliances or intelligent speakers to facilitate a comprehensive reaction.

Such a study could, for example, design and implement IoT devices together with novel security algorithms as an overall prototype of a home safety system aiming to enforce higher level of security. The prototype could then be analysed/tested to assess how effective it is at stopping people breaking into the home.

The research will analyze current home security systems and the potential threats, both existing and proposed against a set of indicators relating to house security systems. For example, this may involve considering the risks and concerns of implementing IoT paradigms in house door locking systems, including hacking or security precautions.

The research would investigate the different safety algorithms and techniques (e.g. encryption, authentication & access control) in order to implement high level security to house door locking system property referred here only as House20System (IServiceCollection). The suitability of using these algorithms in house protection systems, could be measured with the simulation or real test problem solutions. In the end, where research on security mechanism algorithms With IoT For home safety systems reflect insights and approaches to enhance securities of those system further avenues that can be explored for future works..

1.6. Literature Review

Gartner, for example predicted that 8.4 billion connected “things” will be in use worldwide this year and total number would exceed somewhere around 20 billion by 2020 (2017). This exploding wave of billions of IoT devices has sparked serious concerns about the security implications as these types of vulnerability-exposed threat device are often operated in uncontrolled environments and at the risk from such cyber-attacks. HP (2014), in a study, found that 70% of IoT devices are vulnerable to cyber-attacks.

DDoS attacks are one of the popular cyber-attacks, where IoT devices used as zombie machines to flood traffic against your main china and drains it. DDoS attacks saw a 16% increase in Q2 2021 from the previous quarter, with an average of attack duration lasting about (Akamai) A breach of security in home safety systems for example could lead robbers to loot property or threaten occupants among other examples with dire consequences.

A number of security mechanisms and algorithms has been proposed by researchers as well industry professionals to overcome these security challenges. One such study by Wang et al. The method of (2019) introduced a blockchain-based security mechanism for IoT devices. To ensure the integrity of data exchanges between IoT devices, accountants use blockchain technology to function as a decentralized and tamper-free ledger. Al-Fuqaha et al. [39] had first of all further examined the suitability with an additional study A possible solution for the relatively restricted computation facilities and memory footprint of IoT devices as studied by (2015) would be to use lightweight encryption algorithms.

A study by Cho et al. in terms of biometric authentication In ref. [5] authors suggested the use of heart rate variability for identification and its application to IoT devices. Uses the heart rate variability as an authentication signal but it is not only one of these signals that are unforgeable and unique. Another study by Kim et al. Singh et al., (2020) proposed multimodal optimization, which integrates multiple biometric modalities like fingerprint and facial recognition to improve authenticity accuracy and security.

In the case of machine learning algorithms, Ma et al. reviewed this for a study [17]. One of the research work (2019) that has used deep learning algorithms to detect anomalies in network traffic and prevent DDoS attack on IoT devices. The deep learning algorithm could be used to achieve high detection accuracy at 102.93 s and accurate real-time defence against DDoS attacks the findings of this study presented. Effective RAT selection can be seen in works like [11,17] by Garcia-Saavedra et al. On the other hand, Cozzolino et al.(2018) have suggested that we can use reinforcement learning algorithms into securing IoT systems. The results of this work, showed that proposed reinforcement learning algorithm learned the effective defense mechanism for each type or family cyber attacks based on generating strong security policies.

1.6.1. Cybersecurity Risks for IoT-Based Home Safety Systems

Cyber security threats present in IoT-based home safety system are burglary, vandalism or a risk to life of inhabitants. The FBI has reported that home IoT devices are entering attack vectors of cyber-crime and the number of incidents involving Home-IoT Device increased more than 300% over a couple years (FBI,2019). Despite its reputation, most security incidents involving the IoT relate not to devices per se but rather to flaws in software and firmware that cybercriminals can readily exploit.

One of the major cybersecurity dangers for IoT based home security systems is an unauthorized access point from cyber crooks. They may hack a wireless smart lock, instead of gaining control over the door remotely. or they will access a camera to spy on people living inside it. A home alarm system is made up of sensors, like motion detectors or smoke alarms which could also be disabled by hackers and the list goes on. These risks outlined demonstrate that the IoT-based home security systems must be protected by solid security mechanisms and algorithms to protect them from cyber-attacks..

1.6.2. Emerging Technologies for IoT Security

The emergence of new technologies has created a chance to enhance security for IoT-based home safety system [30, 34]. For example, one study by Li et al. Blockchain has been one of the options for designing secure multi-party computation solutions which was suggested to save privacy in home safety systems that access IoT data (2020). Based on multiple forms of blockchain, a security protection mechanism based on homomorphic encryption and secure multi-party computation is proposed to protect the privacy and integrity of IoT data.

Edge Computing: Edge computing is a relatively new technology, but just as IoT itself can be used to help secure our home safety systems. Edge computing processes data at the network edge, near IoT devices rather than sending all of it to a central server for processing and then only transmit either consumed or aggregative results where original raws are no longer wanted nor needed back [14, 15]. This reduces the latency and bandwidth demands on IoT

systems, making IOT data more secure by decreasing the amount of raw unprocessed sensor network information which needs to be transmitted across a possibly insecure wireless communication system [13, 29]. A secure edge computing framework for IoT based home safety systems using lightweight encryption and secure communication protocols to ensure data privacy, integrity has been suggested by Padmaa, Jayasankar [44].

The total number of connected IoT devices will be 30 billion in year Podder, Bukhari [45], Priyadarshini, Kumar [32] and Raghavendar, Batra [33]. The rapid growth of the number of IoT devices in use makes it even more important to develop effective security models and algorithms so that users may be safe and secure, both from a data privacy point-of-view but also reliability. A challenge that often arises regarding the development of security solutions for IoT devices, due to very low computing power and memory, null as appropriate is a minimal amount. Many IoT devices are generally low-power processors and memory-constrained thus making it difficult for intricate security mechanisms to be implemented. Batteries are key, especially if you think about all of the home safety systems that have devices which run on batteries and operate for weeks or months in between charges.

However, much progress has been made in this area as researchers have tried to mitigate the risks by designing several security mechanism and algorithms targeting IoT home safety systems. A study outlined the application of blockchain technology to secure devices in IoT and meter authorized access. The researchers have shown that it is indeed possible to authenticate communication between IoT devices using a blockchain-based access control mechanism.

A few months ago, we discussed research that investigated the use of machine learning algorithms to spot abnormal behavior in IoT devices. With this data, the team trained a neural network to identify abstract patterns associated with IoT device behavior and use that information to recognize behaviors which are likely occurring due to nefarious reasons. The

researchers showed that the same technique could be used for bolstering home safety systems security by detecting arguably nefarious activities earlier in occurring.

Researchers are also developing biometric solutions including facial recognition for enhancing IoT security as an additional layer of your earlier suggestions. Biometric authentication measures are an effective means to tackle the issues of traditional security such as passwords, PINs etc which tend to get compromised.

The deployment of IoT devices in residential settings is growing significantly, based on recent statistics. Statista predicts the worldwide count of smart home devices to grow from 0.3 billion in 2018 (29)1,6(+500%) by increasing to more than a huge amounting everything is expected worth up until that period or would have reached in this type end-of-quarter quarter millions with all such kind things being said ever since against too few towards least one has wondered over other five years 'til we get better and change instead but then possibly even so close whatever sorry guys iIsaid goodbye? it was just once I guess here only because YOU LOVE YOUR hair(which will turn Abdeladi for gods sake onversscity yeah never mind rollover time anyways). And that growth is coming from the rising demand for voice assistants, smart thermostats and security systems — mainstays in modern American homes. With the increasing integration of IoT devices in homes, there is a growing need for robust security protocols to keep out cyber-attacks. One common security measure in the context of IoT devices is employing encryption so that communication among them can occur securely. The use of an algorithm to manipulate data into unreadable information without a decryption key for encoding the likelihood, propagating harder by cybercriminals monitoring out and recovering personal knowledge in real-time.

Apart from encryption, researchers are looking into other novel security approaches for home safety systems which could be manipulated by the IoT revolution. Edge computing, whereby data is processed directly on the device and not transmitted to a centralised cloud server provides an exciting strategy. Using this approach can reduce the amount of data that needs to

be transmitted over net once and for all which also means less vulnerability due to cyber attacks.

It will also be interested in secure IoT firmware. Firmware is the underlying software on the device, and when a firmware vulnerability can be accessed by an attacker or cybercriminal to gain unwarranted access -- that's where it becomes more dangerous. To address this, researchers are researching techniques to secure the firmware such as obfuscating the code of the lime in order to get rid of how easy it is for attacker’s reverse-engineer and examine what was included inside. However, these efforts are still insufficient in making a robust security mechanisms for the development of smart home safety systems based on IoT. A large part of the difficulty comes from a lack of standardization across IoT, as it hinders growth in order to ensure compatibility with every device that may ever connect. A further challenge stems from the fact that a lot of these IoT devices have very little available resources, making it next to impossible in some cases to implement robust security mechanisms.

The home safety system has been the leading application of IoT devices in homes, as per some recent statistics. Grand View Research released a report earlier this year predicting the global smart home security market will rise to $135.6 billion by 2025 at an annual growth rate of 18.9%. Growing consumer worries regarding home security and an appetite for easily operated, connected systems that can be managed remotely are helping to stoke this expansion.

But, these options aren't free from the risk of getting crushed however as with any good thing that grows we know there are increased threats. According to a report from the security vendor Symantec, IoT attacks soared by 300% in 2019 over those of previous years — and the majority of these were aimed at consumer devices like home surveillance cams and routers. This highlights the urgent need for robust security systems to protect against these threats.

In order to overcome them, scientists are investigating a number of routes that could help in enhancing the security aspects of IoT-based home safety systems. They could even employ the use of blockchain technology to add an extra layer of security. How blockchain is a secure and transparent transaction data. Blockchain, as one of the distributed ledger technology (DLT), provide security in making certain records. If this data was stored using the blockchain (instead of however traditional home security systems store it) then a record can be kept that nobody could tamper with, and anyone who is authorized to see the history of events would know exactly what happened.

Additionally, some researchers have proposed the use of artificial intelligence (AI) to help secure IoT devices. For example, using AI algorithms to inspect network traffic for patterns that could indicate a potential cyber-attack. Machine learning can further be applied to automate the identification of security incidents, and thus facilitate faster decision-making during incident response.

Not withstanding these opportunities there are challenges in creating stringent security mechanisms for home safety systems which work on IOT. The IoT ecosystem is vast and comprises multi-home appliances from manufacturers of different brands, leading to privacy integrity within the device itself. Further, security mechanisms should be always under monitoring as the threat landscape is dynamic.

In conclusion, the development of security mechanisms and algorithms for IoT-driven home safety systems can aid in safeguarding users safe as well as private. However, the number of connected IoT devices are also increasing and hence researchers must look for new ways to improve the security posture of these devices. These studies can also help to support the need of implementing strong security mechanisms and algorithms in IoT systems, especially in home safety system. With the increasing number of connected IoT devices, it is important to secure these connections and protect against emerging security threats so they can remain safe for users.

1.7. Research Methodology

Based on the topic of developing mechanism algorithms based on the Internet of Things (IoT) for home automation, a quantitative research methodology can be adopted to investigate the effectiveness of this technology in improving home automation systems. The methodology will involve collecting numerical data through structured instruments such as online surveys, which will be distributed to a large sample of homeowners who have implemented IoT-based home automation systems. The survey will include questions related to the effectiveness of the IoT-based home automation system, the level of user satisfaction, and the benefits and limitations of using this technology. The collected data will undergo analysis using statistical techniques such as correlation and regression analysis, to identify patterns and relationships between variables. The research will also involve ensuring the reliability and validity of the data collection process by using standardized protocols and minimizing potential biases and errors. The results of the research will be used to provide insights into the effectiveness of developing mechanism algorithms based on the IoT for home automation, which can be used to inform future policy and development of this technology. As a part of this research, the following steps will be followed:

- **Define the Research Questions:** The first step would be to define the research questions that will guide the study, such as "What is the effectiveness of developing mechanism algorithms based on the Internet of Things for home automation?". The research question will be derived from an extensive review of the extant literature
- **Develop the Survey Instrument:** The next step would be to develop a survey instrument that will be used to collect data from the sample of homeowners. The survey should be designed to capture data related to the research questions and should be pretested for clarity and ease of use.

- **Recruit Participants:** Once the survey instrument is finalized, participants will be recruited from a variety of sources, such as online communities or homeowner associations. The sample should be representative of the population and should include a minimum of 250 participants to ensure statistical power as estimated from the G-power software.
- **Collect Data:** The survey will be distributed to the participants, and data will be collected on various aspects of the IoT-based home automation system, such as user satisfaction and effectiveness of the technology.
- **Analyze Data:** The collected data will be analyzed using statistical techniques such as correlation, regression analysis and structural equation modelling to identify relationships and patterns between variables.
- **Interpret Results:** The results of the analysis will be interpreted and used to draw conclusions about the effectiveness of developing mechanism algorithms based on the IoT for home automation.
- **Draw Conclusions:** Based on the interpretation of the results, conclusions will be drawn about the effectiveness of the technology and its potential implications for future development and policy.
- **Communicate Findings:** Finally, the findings will be communicated through various channels such as academic publications or conference presentations to share the insights gained from the study with relevant stakeholders.

1.8. References

1. Alowaidi, M., *Fuzzy efficient energy algorithm in smart home environment using Internet of Things for renewable energy resources.* Energy Reports, 2022. **8**: p. 2462-2471.

2. Das, A., S. Chakraborty, and S. Chakraborty, *Where do all my smart home data go? Context-aware data generation and forwarding for edge-based microservices over shared IoT infrastructure.* Future Generation Computer Systems, 2022. **134**: p. 204-218.

3. Hui, T.K.L., R.S. Sherratt, and D.D. Sánchez, *Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies.* Future Generation Computer Systems, 2017. **76**: p. 358-369.

4. Kaur, H., et al., *Intelligent Smart Home Energy Efficiency Model Using Artificial Intelligence and Internet of Things*, in *Artificial Intelligence to Solve Pervasive Internet of Things Issues*. 2021. p. 183-210.

5. Georgia, D., et al., *Evaluation of end user requirements for Smart Home applications and services based on a decision support system.* Internet of Things, 2021. **16**.

6. Gill, S.S., P. Garraghan, and R. Buyya, *ROUTER: Fog enabled cloud based intelligent resource management approach for smart home IoT devices.* Journal of Systems and Software, 2019. **154**: p. 125-138.

7. Krishnamoorthy, R., K. Krishnan, and C. Bharatiraja, *Deployment of IoT for smart home application and embedded real-time control system.* Materials Today: Proceedings, 2021. **45**: p. 2777-2783.

8. Li, W., et al., *Mapping two decades of smart home research: A systematic scientometric analysis.* Technological Forecasting and Social Change, 2022. **179**.

9. Luperto, M., et al., *Seeking at-home long-term autonomy of assistive mobile robots through the integration with an IoT-based monitoring system.* Robotics and Autonomous Systems, 2023. **161**.

10. Minoli, D., *Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach.* Internet of Things, 2020. **10**.

11. Nasir, M., et al., *Enabling automation and edge intelligence over resource constraint IoT devices for smart home.* Neurocomputing, 2022. **491**: p. 494-506.

12. Natarajan, A., V. Krishnasamy, and M. Singh, *Occupancy detection and localization strategies for demand modulated appliance control in Internet of Things enabled home energy management system.* Renewable and Sustainable Energy Reviews, 2022. **167**.

13. Pal, D., X. Zhang, and S. Siyal, *Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach.* Technology in Society, 2021. **66**.

14. Rajesh, P., F.H. Shajin, and G. Kannayeram, *A novel intelligent technique for energy management in smart home using internet of things.* Applied Soft Computing, 2022. **128**.

15. Ramadan, R., et al., *Intelligent home energy management using Internet of Things platform based on NILM technique.* Sustainable Energy, Grids and Networks, 2022. **31**.

16. Agyemang, J.O., et al., *Lightweight rogue access point detection algorithm for WiFi-enabled Internet of Things(IoT) devices.* Internet of Things, 2020. **11**.

17. Ahmad, T. and D. Zhang, *Using the internet of things in smart energy systems and networks.* Sustainable Cities and Society, 2021. **68**.

18. Al-Ward, H., C.K. Tan, and W.H. Lim, *Caching transient data in Information-Centric Internet-of-Things (IC-IoT) networks: A survey.* Journal of Network and Computer Applications, 2022. **206**.

19. Alam, F., et al., *Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT).* Procedia Computer Science, 2016. **98**: p. 437-442.

20. Alavikia, Z. and M. Shabro, *A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey.* Digital Communications and Networks, 2022. **8**(3): p. 388-410.

21. Aljabr, A.A. and K. Kumar, *Design and implementation of Internet of Medical Things (IoMT) using artificial intelligent for mobile-healthcare.* Measurement: Sensors, 2022. **24**.

22. Alulema, D., et al., *SI4IoT: A methodology based on models and services for the integration of IoT systems.* Future Generation Computer Systems, 2023. **143**: p. 132-151.

23. Asha, A., et al., *Optimized RNN-based performance prediction of IoT and WSN-oriented smart city application using improved honey badger algorithm.* Measurement, 2023. **210**.

24. Awan, K.A., et al., *AutoTrust: A privacy-enhanced trust-based intrusion detection approach for internet of smart things.* Future Generation Computer Systems, 2022. **137**: p. 288-301.

25. Bhardwaj, K.K., et al., *Internet of things based smart city design using fog computing and fuzzy logic.* Sustainable Cities and Society, 2022. **79**.

26. Boursianis, A.D., et al., *Internet of Things (IoT) and Agricultural Unmanned Aerial Vehicles (UAVs) in smart farming: A comprehensive review.* Internet of Things, 2022. **18**.

27. Li, J., et al., *Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management.* Energy and AI, 2023. **11**.

28. Li, Y., et al., *Graph-powered learning methods in the Internet of Things: A survey.* Machine Learning with Applications, 2023. **11**.

29. Perez, A.J., et al., *A review of IoT systems to enable independence for the elderly and disabled individuals.* Internet of Things, 2023. **21**.

30. Rejeb, A., et al., *The big picture on the internet of things and the smart city: a review of what we know and what we need to know.* Internet of Things, 2022. **19**.

31. Xiaoyi, Z., et al., *IoT driven framework based efficient green energy management in smart cities using multi-objective distributed dispatching algorithm.* Environmental Impact Assessment Review, 2021. **88**.

32. Priyadarshini, I., et al., *Survivability of industrial internet of things using machine learning and smart contracts.* Computers and Electrical Engineering, 2023. **107**.

33. Raghavendar, K., I. Batra, and A. Malik, *A robust resource allocation model for optimizing data skew and consumption rate in cloud-based IoT environments.* Decision Analytics Journal, 2023.

34. Salim, S., B. Turnbull, and N. Moustafa, *Data analytics of social media 3.0: Privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems.* Ad Hoc Networks, 2022. **128**.

35. Sinha, B.B. and R. Dhanalakshmi, *Recent advancements and challenges of Internet of Things in smart agriculture: A survey.* Future Generation Computer Systems, 2022. **126**: p. 169-184.

36. Sivarajan, S. and S.D. Sundarsingh Jebaseelan, *Efficient adaptive deep neural network model for securing demand side management in IoT enabled smart grid.* Renewable Energy Focus, 2022. **42**: p. 277-284.

37. Lim, H.R., et al., *Smart microalgae farming with internet-of-things for sustainable agriculture.* Biotechnol Adv, 2022. **57**: p. 107931.

38. Liu, L., X. Guo, and C. Lee, *Promoting smart cities into the 5G era with multi-field Internet of Things (IoT) applications powered with advanced mechanical energy harvesters.* Nano Energy, 2021. **88**.

39. Liu, Y., *Simulation of art design of indoor furnishings based on FPGA and internet of things system.* Microprocessors and Microsystems, 2021. **83**.

40. Madhu, B., et al., *Intrusion detection models for IOT networks via deep learning approaches.* Measurement: Sensors, 2023. **25**.

41. Mellit, A. and S. Kalogirou, *Internet of things (IoT) and embedded systems for photovoltaic systems*, in *Handbook of Artificial Intelligence Techniques in Photovoltaic Systems*. 2022. p. 267-329.

42. Menon, V.G., et al., *An IoT-enabled intelligent automobile system for smart cities.* Internet of Things, 2022. **18**.

43. Nizetic, S., et al., *Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future.* J Clean Prod, 2020. **274**: p. 122877.

44. Padmaa, M., et al., *Oppositional chaos game optimization based clustering with trust based data transmission protocol for intelligent IoT edge systems.* Journal of Parallel and Distributed Computing, 2022. **164**: p. 142-151.

45. Podder, A.K., et al., *IoT based smart agrotech system for verification of Urban farming parameters.* Microprocessors and Microsystems, 2021. **82**.